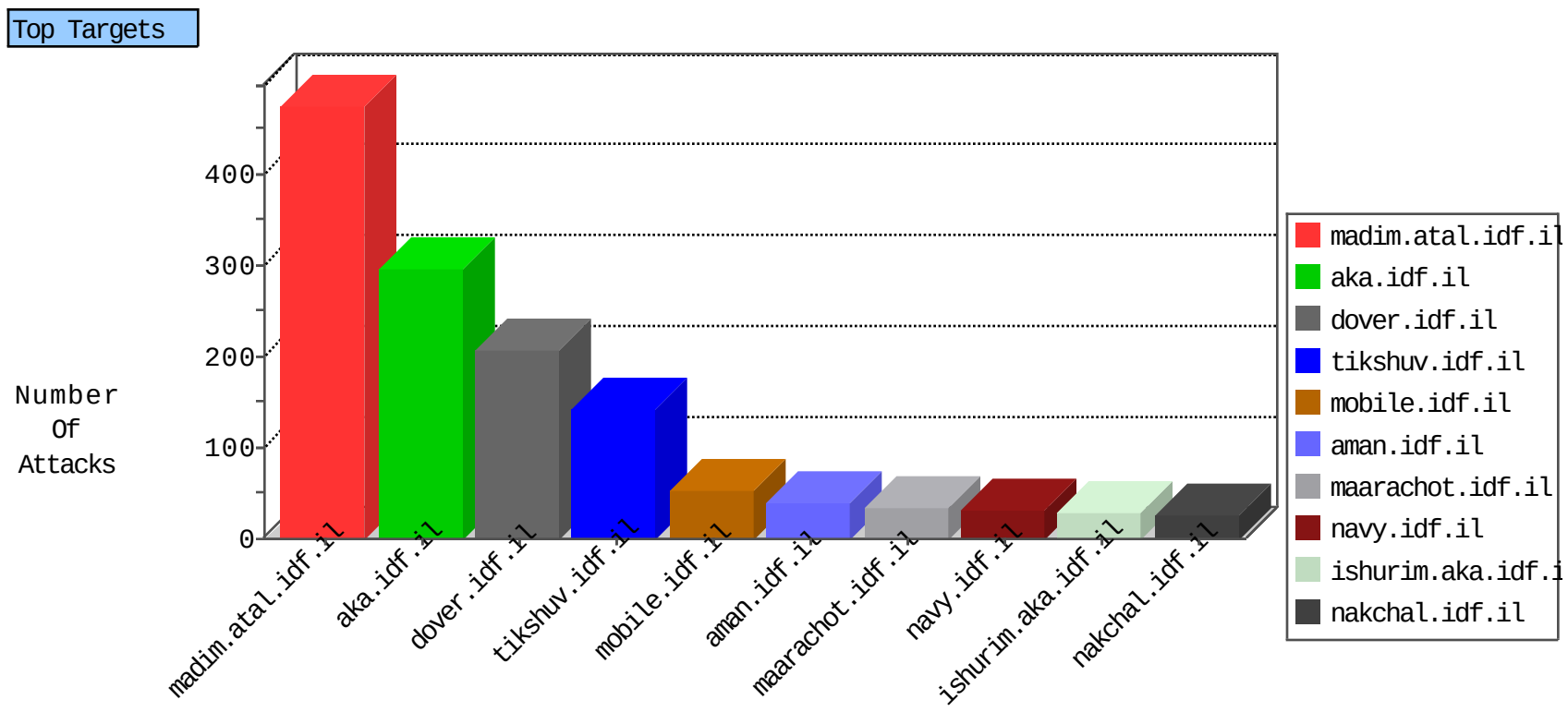
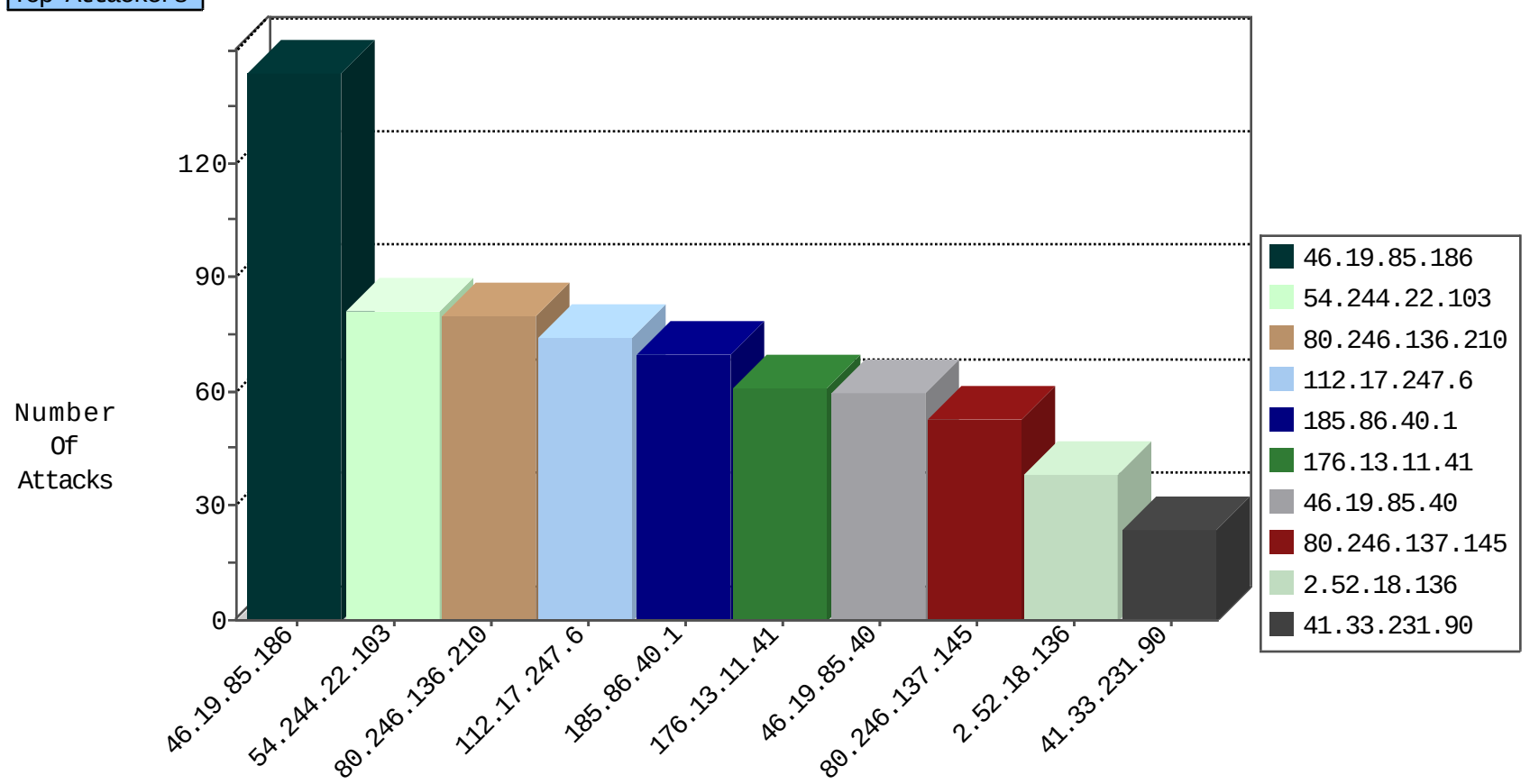
02-11-2016-10:04:01 to 02-11-2016-11:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-11-2016-10:04:01 to 02-11-2016-11:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.154.88.39	Israel	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
114.85.34.73	China	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
188.138.1.218	Germany	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1

02-11-2016-10:04:01 to 02-11-2016-11:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
88.248.98.197	Turkey	147.237.77.170	maarachot.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	14
77.127.236.87	Israel	147.237.77.170	maarachot.idf.il	C122: HTTP: Access to - .exe or .dll	Permit	2

02-11-2016-10:04:01 to 02-11-2016-11:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
77.127.236.87	147.237.77.170	Israel	maarachot.idf.il	WEB-FRONTPAGE /_vti_bin/ access	3
46.120.160.95	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.168.227.138	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
212.29.211.62	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.210.216.68	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
91.228.248.251	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.135.161	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.110.24	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.126.94.156	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.1.173.200	147.237.0.33	Turkey	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
213.57.231.135	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.115.85.113	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.3.74	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.117.208.243	147.237.76.31		nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.64.68	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1

02-11-2016-10:04:01 to 02-11-2016-11:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	70
46.19.85.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	60
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
109.253.215.38	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
79.179.117.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.86.119	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.64.255.235	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.10.115	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	11
65.55.215.223	United States	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
81.218.192.106	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.86.131	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.118.12.102	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
212.68.153.181	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	9
192.118.12.102	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.85.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
194.90.119.123	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
66.102.9.3	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	7
2.54.56.120	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.86.28	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.26.147.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.176	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
180.153.81.159	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.102.254.176	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.219.98.102	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.93	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.126	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.134	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
46.19.85.126	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.178.200.40	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
46.19.85.134	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.192	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.126	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
212.179.21.194	Israel	147.237.77.170	maarachot.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.126	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.94.126.154	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
84.95.252.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.124.14	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.207.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.76.127.219	Israel	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
80.179.114.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.106.49	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.11.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.48.205	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3

02-11-2016-10:04:01 to 02-11-2016-11:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	101
80.246.136.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	76
185.86.40.1		147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 185.86.40.1	Block	69
176.13.11.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
80.246.137.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
46.19.85.186	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.186	Block	43
2.52.18.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
112.17.247.6	China	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	37
112.17.247.6	China	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	37
2.54.48.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
80.246.136.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
80.246.137.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
80.246.136.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
80.246.138.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
46.19.86.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.253.215.38	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
80.246.136.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
80.246.136.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
109.253.141.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.119	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.54.55.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.156.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.127.236.87	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 77.127.236.87	Block	3
46.19.86.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 217.194.198.104 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	2
95.86.68.164	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 95.86.68.164	Block	2
2.54.161.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.127.236.87	Israel	147.237.77.170	maarachot.idf.il	Multiple _vti_ from 77.127.236.87	Block	2
136.243.67.234	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	2
46.116.23.40	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation searchText in www.refua.atal.idf.il/994-he/refuah.aspx	Block	2
79.182.139.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
87.69.180.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.14.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
165.91.12.68	United States	147.237.72.166	aka.idf.il	Distributed NULL Character in Method	Block	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx	Block	1
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method Âœ	Block	1
123.125.71.16	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/3203.pdf	Block	1
212.179.3.44	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
94.137.173.134	Georgia	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
184.105.139.68	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
79.176.109.136	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	1
157.55.39.39	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
46.120.70.149	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
212.179.3.44	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
37.142.203.114	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
212.179.3.44	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
173.252.115.86	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/1143-he/atal.aspx&ved=0ahukewjt75dpou_kahxdqbqkhfwybbyqfggkmai&usg=afqjcngqjkbeqgwvwbr0rirunrhauekoaq&sig2=ixf57ystoltfm6gpiky3lg	Block	1
80.179.40.62	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL ÂœÖ¼zqÂ´[[#6]]bâ€”2â€?×±6:\w•l}â€?ÂŸ9[[#28]]1Â»[[#14]]â€¢×¨â‚¬×¨â,¬[[#26]][[#6]]ÂŽÂ?Âœ×'•[[#14]];ÂŠ ÃŸ-×²×¥Ö±×šrÂ¸â‚¬×¨â,¬[[#26]]Ã—[[#6]]pd5×ŸuÃŠ×¤Â®×“Ãš6â‚ªâ€ºâ€žg;}ÃšÂ[[#20]]_\Â´mâ‚ªbf,6mzf[[#6]]â€”×•vÂ?×˜Â±[[#14]]Ö·Æ'Â¹[[#2]]Â·oâ€˜[[#19]]×Ÿ8[[#17]]×€r× â„¢×žca[[#31]]~z4Âœy1tÖ¹[[#27]]Ã›×”[[#12]]nt×¨1hbÖ´&Ö» @×™gÂ¢Ã·Â¿Â?k#×?`[[#16]]	Block	1

02-11-2016-10:04:01 to 02-11-2016-11:04:01